Terms used **IP core obfuscation scramble entangle** Found **40** of **201,062**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 40 Result page: **1** 2 3 next

Relevance scale

1 Software and languages: Proteus: virtualization for diversified tamper-resistance
Bertrand Anckaert, Mariusz Jakubowski, Ramarathnam Venkatesan
October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**
Publisher: ACM Press
Full text available: pdf(299.79 KB) Additional Information: full citation, abstract, references, index terms

Despite huge efforts by software providers, software protection mechanisms are still broken on a regular basis. Due to the current distribution model, an attack against one copy of the software can be reused against any copy of the software. Diversity is an important tool to overcome this problem. It allows for renewable defenses in space, by giving every user a different copy, and renewable defenses in time when combined with tailored updates. This paper studies the possibilities and limitation ...

Keywords: copyright protection, diversity, intellectual property, obfuscation, tamper-resistance, virtualization

2 Selected writings on computing: a personal perspective
Edsger W. Dijkstra
January 1982 Book
Publisher: Springer-Verlag New York, Inc.
Full text available: pdf(60.98 MB) Additional Information: full citation, abstract, references, cited by, index terms

Since the summer of 1973, when I became a Burroughs Research Fellow, my life has been very different from what it had been before. The daily routine changed: instead of going to the University each day, where I used to spend most of my time in the company of others, I now went there only one day a week and was most of the time that is, when not travelling!-- alone in my study. In my solitude, mail and the written word in general became more and more important. The circumstance that my employe ...

3 Attacks and countermeasures: Diversify sensor nodes to improve resilience against node compromise
Abdulrahman Alarifi, Wenliang Du
October 2006 **Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks SASN '06**
Publisher: ACM Press

within the duration during which the secured rules related to manufacture of integrated circuits may be processed.

15. The method of claim 11, wherein the secured rules related to manufacture of integrated circuits is not unlocked until determining that the current period is within the duration during which the secured rules related to manufacture of integrated circuits may be processed.

16. The method of claim 11, wherein the duration during which the secured rules related to manufacture of integrated circuits may be processed is different for different portions of the secured rules related to manufacture of integrated circuits.

17. The method of claim 11, wherein the duration during which the secured rules related to manufacture of integrated circuits may be processed is different for different users.

18. A system for secured exchange of electronic design automation information comprising an electronic design automation tool operational for:

receiving a file comprising secured electronic design automation information;

identifying the secured electronic design automation information within the file;

determining whether one or more conditions for accessing at least some portion of the secured electronic design automation information within the file have been met; and

accessing the at least some portion of the secured electronic design automation information to process the at least some portion of the secured electronic design automation information without revealing the at least some portion of the secured electronic design automation information.

19. The method of claim 18, wherein data related to the one or more conditions for accessing the at least some portion of the secured electronic design automation information is specified within the file comprising the secured electronic design automation information.

20. The system of claim 18 further comprising:

a server computer operational for providing the electronic design automation tool with one or more keys for accessing the at least some portion of the secured electronic design automation information; and

in response to a call back request from the electronic design automation tool, providing the electronic design automation tool with data confirming whether the one or more conditions for accessing the at least some portion of the secured electronic design automation information have been met.

* * * * *

Full text available: pdf(767.29 KB) Additional Information: full citation, abstract, references, index terms

A great challenge in securing sensor networks is that sensor nodes can be physically compromised. Once a node is compromised, attackers can retrieve secret information (e.g. keys) from the node. In most of the key pre-distribution schemes, the compromise of secret information on one node can have substantial impact on other nodes because secrets are shared by more than one node in those schemes. Although tamper-resistant hardware can help protect those secrets, it is still impractical for sensor ...

Keywords: diversity, obfuscation, reverse engineering, wireless sensor networks

4 Software issues: Control flow based obfuscation
Jun Ge, Soma Chaudhuri, Akhilesh Tyagi
November 2005 **Proceedings of the 5th ACM workshop on Digital rights management DRM '05**
Publisher: ACM Press
Full text available: pdf(316.58 KB) Additional Information: full citation, abstract, references, index terms

A software obfuscator is a program O to transform a source program *P* for protection against malicious reverse engineering. O should be *correct* (O(*P*) has same functionality with *P*), *resilient* (O(*P*) is resilient against attacks), and *effective* (O(*P*) is not too much slower than *P*). In this paper we describe the design of an obfuscator which consists of two parts. The first part extracts the control flow information from the program and ...

Keywords: control flow, software obfuscation

5 Intrusion detection: Randomized instruction set emulation to disrupt binary code injection attacks
Elena Gabriela Barrantes, David H. Ackley, Trek S. Palmer, Darko Stefanovic, Dino Dai Zovi
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: pdf(160.71 KB) Additional Information: full citation, abstract, references, citings, index terms

Binary code injection into an executing program is a common form of attack. Most current defenses against this form of attack use a 'guard all doors' strategy, trying to block the avenues by which execution can be diverted. We describe a complementary method of protection, which disrupts foreign code execution regardless of how the code is injected. A unique and private machine instruction set for each executing program would make it difficult for an outsider to design binary attack code against ...

Keywords: automated diversity, emulation, information hiding, language randomization, obfuscation, security

6 Session 2: Review and analysis of synthetic diversity for breaking monocultures
James E. Just, Mark Cornwell
October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode WORM '04**
Publisher: ACM Press
Full text available: pdf(356.14 KB) Additional Information: full citation, abstract, references, citings, index terms

The increasing monoculture in operating systems and key applications and the enormous expense of N-version programming for custom applications mean that lack of diversity is a fundamental barrier to achieving survivability even for high value systems that can afford hot spares. This monoculture makes flash worms possible. Our analysis of vulnerabilities and exploits identifies key assumptions required to develop successful attacks. We review the literature on synthetic diversity techniques, f ...

Keywords: diversity, n-version programming, vulnerability

7 Randomized instruction set emulation
Elena Gabriela Barrantes, David H. Ackley, Stephanie Forrest, Darko Stefanović
February 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 1
Publisher: ACM Press
Full text available: pdf(374.44 KB) Additional Information: full citation, abstract, references, citings, index terms

Injecting binary code into a running program is a common form of attack. Most defenses employ a "guard the doors" approach, blocking known mechanisms of code injection. *Randomized instruction set emulation* (RISE) is a complementary method of defense, one that performs a hidden randomization of an application's machine code. If foreign binary code is injected into a program running under RISE, it will not be executable because it will not know the proper randomization. The pape ...

Keywords: Automated diversity, randomized instruction sets, software diversity

8 Manufacturing cheap, resilient, and stealthy opaque constructs
Christian Collberg, Clark Thomborson, Douglas Low
January 1998 **Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '98**
Publisher: ACM Press
Full text available: pdf(1.59 MB) Additional Information: full citation, references, citings, index terms

9 Session 14A: Correcting errors without leaking partial information
Yevgeniy Dodis, Adam Smith
May 2005 **Proceedings of the thirty-seventh annual ACM symposium on Theory of computing STOC '05**
Publisher: ACM Press
Full text available: pdf(246.44 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper explores what kinds of information two parties must communicate in order to correct errors which occur in a shared secret string W. Any bits they communicate must leak a significant amount of information about W --- that is, from the adversary's point of view, the entropy of W will drop significantly. Nevertheless, we construct schemes with which Alice and Bob can prevent an adversary from learning any *useful* information about W. Specifically, if the entropy of W is sufficientl ...

Keywords: bounded storage model, code obfuscation, cryptography, entropic security, error-correcting codes, information reconciliation, randomness extractors

10 Software watermarking: models and dynamic embeddings
Christian Collberg, Clark Thomborson
January 1999 **Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '99**

Publisher: ACM Press
Full text available: pdf(2.19 MB) Additional Information: full citation, references, citings, index terms

11 Intrusion detection: Packet vaccine: black-box exploit detection and signature generation
XiaoFeng Wang, Zhuowei Li, Jun Xu, Michael K. Reiter, Chongkyung Kil, Jong Youl Choi
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(451.38 KB) Additional Information: full citation, abstract, references, index terms

In biology,a *vaccine* is a weakened strain of a virus or bacterium that is intentionally injected into the body for the purpose of stimulating antibody production.Inspired by this idea, we propose a packet vaccine mechanism that randomizes address-like strings in packet payloads to carry out fast exploit detection, vulnerability diagnosis and signature generation. An exploit with a randomized jump address behaves like a vaccine: it will likely cause an exception in a vulnerable program's p ...

Keywords: black-box defense, exploit detection, signature generation, vaccine injection, worm

12 Reviewed articles: The devil and packet trace anonymization
Ruoming Pang, Mark Allman, Vern Paxson, Jason Lee
January 2006 **ACM SIGCOMM Computer Communication Review**, Volume 36 Issue 1
Publisher: ACM Press
Full text available: pdf(119.06 KB) Additional Information: full citation, abstract, references, index terms

Releasing network measurement data---including packet traces---to the research community is a virtuous activity that promotes solid research. However, in practice, releasing anonymized packet traces for public use entails many more vexing considerations than just the usual notion of how to scramble IP addresses to preserve privacy. Publishing traces requires carefully balancing the security needs of the organization providing the trace with the research usefulness of the anonymized trace. In thi ...

13 Folklore confirmed: reducible flow graphs are exponentially larger
Larry Carter, Jeanne Ferrante, Clark Thomborson
January 2003 **ACM SIGPLAN Notices , Proceedings of the 30th ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '03**, Volume 38 Issue 1
Publisher: ACM Press
Full text available: pdf(204.49 KB) Additional Information: full citation, abstract, references, index terms

Many program analysis techniques used by compilers are applicable only to programs whose control flow graphs are *reducible*. Node-splitting is a technique that can be used to convert any control flow graph to a reducible one. However, as has been observed for various node-splitting algorithms, there can be an exponential blowup in the size of the graph.We prove that exponential blowup is unavoidable. In particular, we show that any reducible graph that is equivalent to the complete graph o ...

Keywords: compilers, computational complexity, programming languages, safety/security in digital systems

14 KDD-Cup 2000 organizers' report: peeling the onion
Ron Kohavi, Carla E. Brodley, Brian Frasca, Llew Mason, Zijian Zheng
December 2000 **ACM SIGKDD Explorations Newsletter**, Volume 2 Issue 2
Publisher: ACM Press
Full text available: pdf(855.71 KB) Additional Information: full citation, citings, index terms

Keywords: KDD-Cup, best practices, competition, data cleansing, data mining, e-commerce, insight, peeling the onion, real-world data

15 A tentative approach to constructing tamper-resistant software
Masahiro Mambo, Takanori Murayama, Eiji Okamoto
January 1998 **Proceedings of the 1997 workshop on New security paradigms NSPW '97**
Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, references, index terms

16 Columns: Risks to the public in computers and related systems
Peter G. Neumann
January 2001 **ACM SIGSOFT Software Engineering Notes**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(3.24 MB) Additional Information: full citation

17 Session 3: A type system extension for middleware interactions
Sven De Labey, Eric Steegmans
March 2007 **Proceedings of the 1st workshop on Middleware-application interaction: in conjunction with Euro-Sys 2007 MAI '07**
Publisher: ACM Press
Full text available: pdf(462.32 KB) Additional Information: full citation, abstract, references, index terms

Object-oriented programming languages such as Java provides inadequate support for advanced method invocation strategies in distributed applications. Invocation semantics such as *reliable unicast* and *multicast* must be implemented based on primitive, unreliable unicast mechanisms such as Java RMI and Socket communication. This forces developers to devise ad hoc communication strategies, which is a repetitive and error-prone process. Moreover, these communication strategies are en ...

Keywords: fault tolerance, group method invocation, type qualifier, type system

18 Behavioral synthesis techniques for intellectual property protection
Farinaz Koushanfar, Inki Hong, Miodrag Potkonjak
July 2005 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 10 Issue 3
Publisher: ACM Press
Full text available: pdf(439.81 KB) Additional Information: full citation, abstract, references, index terms

We introduce dynamic watermarking techniques for protecting the value of intellectual property of CAD and compilation tools and reusable design components. The essence of the new approach is the addition of a set of design and timing constraints which encodes the author's signature. The constraints are selected in such a way that they result in a minimal hardware overhead while embedding a unique signature that is difficult to remove and forge. Techniques are applicable in conjunction with an ar ...

Keywords: Intellectual property protection, behavioral synthesis, watermarking

19 Security: Hardware support for code integrity in embedded processors
Milena Milenković, Aleksandar Milenković, Emil Jovanov
September 2005 **Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems CASES '05**
Publisher: ACM Press
Full text available: pdf(371.76 KB) Additional Information: full citation, abstract, references, index terms

Computer security becomes increasingly important with continual growth of the number of interconnected computing platforms. Moreover, as capabilities of embedded processors increase, the applications running on these systems also grow in size and complexity, and so does the number of security vulnerabilities. Attacks that impair code integrity by injecting and executing malicious code are one of the major security issues. This problem can be addressed at different levels, from more secure softwa ...

Keywords: attacks, code injection, code integrity

20 Short papers: Crocus: a steganographic filesystem manager
Hioki Hirohisa
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(83.25 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic filesystems are widely used to protect private files. It is, however, impossible to hide the existence of private information by such filesystems. Steganographic filesystems attempt to address this problem by embedding files imperceptibly into containers. In most steganographic filesystems ever proposed, files are embedded into containers those apparently randomized. Their existence would, however, imply that they include hidden files. This paper presents a new steganographic files ...

Keywords: filesystem manager, steganography

Results 1 - 20 of 40 Result page: **1** 2 3 next